Załącznik nr 1 do zapytania ofertowego

**Opis przedmiotu zamówienia**

1. Przedmiotem zamówienia jest usługa przeprowadzenia testów bezpieczeństwa polegająca na weryfikacji skuteczności ochrony systemów teleinformatycznych MRiT.

Testy bezpieczeństwa dotyczyć będą weryfikacji ochrony technicznej systemów (testy penetracyjne – lit. A), aplikacji oraz infrastruktury informatycznej, optymalizacji ich bezpieczeństwa(audyty bezpieczeństwa – lit. B), a także z uwzględnieniem doradztwa w tym zakresie, potwierdzone każdorazowo raportami z przeprowadzonych czynności testowych (raporty z testów – lit. C), a która została wykonana przez osoby o odpowiednich kompetencjach merytorycznych (wymagane kompetencje – lit. D).

1. Planowane świadczenie usług testów bezpieczeństwa będzie obejmowało 10 roboczodni
w miesiącu i będzie następowało zgodnie z zapotrzebowaniem Zamawiającego, realizowanym przez cały okres trwania umowy.
2. Umowa dotycząca usług testów bezpieczeństwa zostanie zawarta na okres 12 miesięcy, będzie rozliczana w cyklu miesięcznym na podstawie liczby przepracowanych roboczo-dni, w oparciu
o podpisane w danym miesiącu protokoły odbioru wykonanych usług.

**Szczegółowy opis przedmiotu zamówienia**

Zamawiana usługa testów bezpieczeństwa będzie uwzględniała typy, zakres oraz metodykę zgodnie
z poniższymi wytycznymi.

1. **Testy penetracyjne**
2. Usługa testów penetracyjnych musi poddawać ocenie oraz wskazywać podatności w co najmniej następujących obszarach dotyczących:
3. mechanizmów uwierzytelniania – weryfikując skuteczność procesu uwierzytelniania oraz wskazując podatności występujące w tym obszarze,
4. zarządzania sesją – weryfikując skuteczność mechanizmów zarządzania sesją użytkownika oraz wskazując możliwe podatności występujące w tym obszarze,
5. skuteczności walidacji danych – badając skuteczność użytych mechanizmów walidacyjnych oraz oceniając ich adekwatność, zarówno w zakresie walidacji rodzaju danych jak i ich rozmiaru czy dopuszczalnych ilości wprowadzanych danych wraz z identyfikacją podatności w tym obszarze,
6. stosowanych algorytmów kryptograficznych – weryfikując skuteczność oraz zgodność ze standardami (np. NIST) w zakresie zastosowanych mechanizmów ochrony kryptograficznej (np. TLS, funkcje skrótu – ang. *hash*, algorytmy szyfrujące i deszyfrujące, podpisywanie), ocena skuteczności wykorzystania certyfikatów i serwerów certyfikatów oraz identyfikacja podatności w tym zakresie,
7. obsługi błędów – podając ocenie poprawność obsługi błędów/wyjątków powstających na skutek użytkowania testowanego rozwiązania jak również wskazanie potencjalnych podatności w tym obszarze,
8. zapewnienia ochrony danych (poufność, rozliczalność, integralność) – weryfikując mechanizmy przetwarzania danych, ze szczególnym uwzględnieniem danych osobowych, w identyfikacji możliwości nieautoryzowanego dostępu i/lub modyfikacji jak również oceniać mechanizmy audytu prowadzonych na tych danych operacji(rozliczalność),
9. bezpieczeństwa komunikacji (na poziomie warstwy trzeciej - sieciowej i czwartej – aplikacyjnej modelu OSI, podział na strefy sieciowe np. DMZ) - weryfikując zastosowania oraz skuteczności dobrania zabezpieczeń sieciowych oraz usług sieciowych takich jak np. Firewall, Web Application Firewall, Proxy oraz wykrycie ewentualnych podatności w tym obszarze, a także weryfikacja separacji na poziomie sieciowej poprzez wydzielenie stref bezpieczeństwa takich jak np. DMZ, sieci administracyjnych, sieci połączeń między warstwami aplikacji, a także oceniając bezpieczeństwo w zakresie dostępu poprzez mechanizmy VPN,
10. przeciążenia systemu – oceniając skuteczność ochrony systemu przed przeciążeniem lub innym błędnym działaniem związanych przez nieuprawniony wzrost obciążenia systemu jak również wskazanie potencjalnych podatności,
11. bezpieczeństwa kodu źródłowego – polegając na analizie statycznej kodu z wykorzystaniem narzędzi automatyzujących wykonawcy wraz z manualnym wsparciem w zakresie weryfikacji wykrytych nieprawidłowości, wykonywane w środowisku zamawiającego,
12. wykrywanie usług sieciowych udostępnionych w Internecie – polegające na identyfikowaniu i badaniu usług i źródeł usług wystawionych do sieci Internet, jak również identyfikowaniu podatności w obrębie tych usług,
13. wykrywania infekcji szkodliwym oprogramowaniem (np. wykrywanie malware, programów wyłudzających, programów typu exploit, backdoor ) – weryfikując bezpieczeństwo danych (np. plików komputerowych) oraz oprogramowania, a polegająca na wykrywaniu i eliminacji zagrożeń wynikających z infekcji szkodliwym oprogramowaniem, a także polegające na eliminacji błędnych identyfikacji zagrożenia (ang. False-positive),
14. zapewniania bezpieczeństwa oprogramowania bazowego (np. systemu operacyjny, firmware, kontenerów aplikacji np. JBOSS) - poddająca ocenie aktualność oraz odporność na znane zagrożenia wykorzystanego oprogramowania bazowego takiego jak na przykład system operacyjny(linux, Windows), Firmware (np. infrastruktura sieciowa), tomcat, JBOSS, a także oceniająca skuteczność konfiguracji w zakresie bezpieczeństwa (np. włączone usługi sieciowe, identyfikujące wymagane aktualizacje w obszarze bezpieczeństwa, poprawność działania mechanizmów zapewniających rozliczalność (np. logi audytowe, logi techniczne) , poprawność działania systemów backupu,
15. zapewniania bezpieczeństwa urządzeń i sieci przewodowych,
16. zapewniania bezpieczeństwa urządzeń i sieci bezprzewodowych (zarówno GSM jak i Wi-Fi) – polegająca na weryfikacji konfiguracji urządzeń komunikacji bezprzewodowej takich jak Access- Pointy oraz urządzenia klienckie - przenośne wraz z identyfikacją podatności w tym zakresie.
17. Realizacja usługi testów penetracyjnych będzie polegała na wykrywaniu podatności technicznych w oparciu o testy typu „Black box” – tester nie posiada wiedzy dotyczącej testowanego obiektu.
18. Realizacja usługi testów penetracyjnych będzie polegać na wykrywaniu podatności technicznych co najmniej uwzględniając przy tym sposoby takie jak:
19. modyfikacja adresu URL – modyfikacja odwołań do usług sieciowych(serwisów), polegających na zmianie składni lub zawartości łańcucha URL,
20. wprowadzanie niedozwolonych plików – wprowadzenie za pośrednictwem formularzy lub innych metod niedozwolonych plików lub danych, w tym
21. wprowadzaniu niedozwolonej treści – (np. Cross-Site Scripting),
22. wywołania niedozwolonej akcji (np. Cross-Site Request Forgery),
23. przechwytywanie komunikacji (Man in The Middle),
24. utrata poufności danych (SQL Injection, nieuprawniony dostęp do kodu źródłowego, Code Injection),
25. nieuprawnione, zagrażające działania na XML (XML External Entity, XML Bomb),
26. nieuprawniony dostęp do katalogów – wywoływanie funkcji trawersujących po niedozwolonych ścieżkach katalogowych z danymi (np. systemowymi),
27. przepełnienie buforów/stosu – przerwanie działania oprogramowania często na skutek przeprowadzenia niedozwolonej operacji,
28. identyfikacja szkodliwego oprogramowania – identyfikacja oprogramowania stanowiącego zagrożenia dla poufności i integralności danych, z uwzględnieniem mechanizmu eliminacji błędnych wykryć takiego oprogramowania (ang. False-Positive), wraz z korektami u dostawców skanerów oprogramowania.
29. Wymagania dotyczące sposobu oraz zakresu realizacji usługi testów penetracyjnych muszą obejmować:
30. wykorzystanie informacji z baz danych o podatnościach, z uwzględnieniem co najmniej jednej z udostępnianych przez: SANS INSTITUTE (sans.org) , NIST (nist.gov – NVD), a także CVE – Common Vulnarabilities and Exposures (mitre.org), Web Application Security Consortium (webappsec.org) lub innych uznanych przez Zamawiającego jako równoważne,
31. stosowanie co najmniej jednego ze standardów w zakresie testów bezpieczeństwa takich jak wytyczne: organizacji OWASP (owasp.org) – Open Web Application Security Project (ASVS), OSSTMM (isecom.org) – Open Source Security Testing Methodology Manual, PTES (pentest – standard.org) – Penetration Testing Execution Standards, NIST (nist.org) –
w zakresie testów penetracyjnych lub innych uznanych przez Zamawiającego jako równoważne,
32. umiejętności stosowania list kontrolnych w oparciu o uznane w zakresie bezpieczeństwa organizacje takie jak NIST (nist.gov), NSA (nsa.gov), CIS (cisecurity.org), US-CCU (us-ccu.us),
33. formalne dokumentowanie wykonywanych testów na każdym etapie ich trwania.
34. [*Usługi mogą zostać zlecone przez Zamawiającego w przypadku oddelegowania przez Wykonawcę do realizacji zamówienia osób posiadających wymagane kompetencje i doświadczenie i uzyskania przez Wykonawcę punktów w kryterium „Testy bezpieczeństwa fizycznego”*] Testy bezpieczeństwa fizycznego polegające na ocenie odporności Zamawiającego na próby nieautoryzowanego fizycznego dostępu do pomieszczeń.
35. **Audyt bezpieczeństwa oraz wsparcie projektowe**
36. Audyt bezpieczeństwa oraz wsparcie projektowe architektury systemów i aplikacji IT obejmujący:
37. audyt przyjętych wariantów i zasad dotyczących warstwowości systemu i aplikacji zgodnie z modelem 1,2 lub 3 –warstwowym (prezentacja, logika i dane),
38. audyt warstw systemów i aplikacji oraz wsparcie projektowe w zakresie bezpieczeństwa w tym w szczególności weryfikacja:
39. mechanizmów uwierzytelniania – autentykacji, autoryzacji oraz w zakresie rozliczalności,
40. bezpieczeństwa komunikacji (np. szyfrowanie w warstwie trzeciej i czwartej modelu OSI, podpisywanie komunikatów(np. XML),
41. mechanizmów walidacyjnych (weryfikacja danych wejściowych pod kątem zawartości składni, rozmiaru oraz z uwzględnieniem czynnika czasu - np. ilość zapytań w jednostce czasu),
42. audyt sposobów oraz wsparcie na etapie projektowania systemów i aplikacji w celu zapewnienia poufności i integralności danych wraz zachowaniem ich rozliczalności,
43. audyt architektury oraz wsparcie na etapie jej opracowywania w zakresie skalowalności systemu i aplikacji, zarówno w zakresie wolumenu danych jak i jednoczesności wykonywanych operacji
44. audyt architektury,
45. audyty bezpieczeństwa mechanizmów przeciwdziałania wyciekom informacji (ang. *Data Leak Protection* – DLP),
46. Audyt bezpieczeństwa sieci oraz usług sieciowych oraz wsparcie na etapie ich projektowania ze szczególnym uwzględnieniem:
47. mechanizmów separacji sieci, także w zakresie segmentacji oraz reguł sieciowych firewall w warstwie 2, 3 i czwartej modelu OSI,
48. mechanizmów zapewnienia bezpieczeństwa sieci bezprzewodowych GSM oraz Wi-Fi,
49. audyty bezpieczeństwa mechanizmów przeciwdziałania wyciekom informacji (ang. *Data Leak Protection* – DLP),
50. mechanizmów ochrony proaktywnej takich jak systemy IPS, IDS (ang. *Intrusion Prevention/Detection System*) oraz systemy korelacyjnej analizy zdarzeń.
51. Audyt bezpieczeństwa baz danych oraz wsparcie na etapie projektowania systemów bazodanowych ze szczególnym uwzględnieniem mechanizmów uwierzytelniania (poufności), obejmujący mechanizmy uprawnień na poziomie bazy danych, w tym schematów, kolumn oraz procedur, a także w zakresie rozliczalności i integralności danych oraz wydajności i skalowalności wraz z uwzględnieniem mechanizmów ochrony proaktywnej takich jak systemy zarządzania dostępem do danych (ang. *database access management* – DAM),
52. Audyt bezpieczeństwa urządzeń końcowych wraz ze wsparciem dotyczącym opracowywania polityk bezpieczeństwa dla tych urządzeń, uwzględniających rodzaj przetwarzanych danych, uprawnienia użytkowników oraz z uwzględnieniem aspektów dotyczących bezpieczeństwa poczty elektronicznej, dostępu do sieci Internet, ochrony antywirusowej oraz ochrony przed innego rodzaju atakami (np. socjotechnicznymi, żądaniami okupu – ransomware),
53. Audyt bezpieczeństwa systemów operacyjnych oraz oprogramowania bazowego firmware jak również konsultacje na etapie projektowym (w tym wyboru rozwiązania) w zakresie zabezpieczania (ang. *hardening*), podziału przestrzeni pamięci RAM oraz pamięci dyskowej, weryfikacji aktualności oprogramowania bazowego oraz systemu operacyjnego wraz ze wszystkimi zainstalowanymi komponentami, ocena przyjętych mechanizmów rozliczalności działań użytkowników, operatorów oraz administratorów tych systemów wraz z oceną adekwatności przyznanych uprawnień,
54. Audyt bezpieczeństwa w zakresie zasad backupu i archiwizacji danych z uwzględnieniem wymagań w zakresie parametrów przywrócenia do działania po awarii (ang. *RTO, RPO, MTD*).
55. [Usługi mogą zostać zlecone przez Zamawiającego w przypadku oddelegowania przez Wykonawcę do realizacji zamówienia osób posiadających wymagane kompetencje
i doświadczenie i uzyskania przez Wykonawcę punktów w kryterium „Audyt bezpieczeństwa fizycznego”] Audyt bezpieczeństwa fizycznego
56. ocena architektury systemu kontroli dostępu,
57. ocena architektury systemu nagrywania wizyjnego (telewizji dozorowej)

Zamawiana usługa testów bezpieczeństwa będzie uwzględniała sposób raportowania prac oraz kompetencje zespołu testujące zgodnie z poniższymi zapisami.

1. **Raportowanie wykonanych prac w ramach zleconych usług**

Raport z wykonanych usług będzie wykonywany każdorazowo po przeprowadzonych testach oraz musi co najmniej obejmować informacje takie jak:

1. Informacje dla kierownictwa - streszczenie najważniejszych kwestii związanych i wynikających z przeprowadzonych testów takich jak przedmiot i cel testów wraz z wynikiem, a także zwięzłe rekomendacje,
2. Informacje szczegółowe opisujące co najmniej:
3. opis testowanego przedmiotu,
4. zakres prowadzonych testów,
5. cel prowadzonych testów,
6. przyjęte założenia oraz metodyka/sposób testowania (wraz z uzasadnieniem)
7. przebieg testów (wraz ze wszystkimi zapiskami powstałymi w procesie testowania)
8. obserwacje i ustalenia - opis sytuacji (zawierające także przyczyny występujących błędów i podatności oraz potencjalny wektor ataku ),
9. wyniki przeprowadzonych testów – wskazanie podatności wraz ich ważnością,
10. wnioski – ocena badanego obszaru wraz z kryterium ważności (poziomu zagrożenia),
11. rekomendacje – zalecane zmiany wraz ze wskazaniem miejsc oraz propozycją ich implementacji,
12. W przypadku oceny kodów źródłowych testy powinny wskazać na źródło błędu, interpretację (ocenę potencjalnych skutków, potencjalny wektor ataku) oraz uwzględniać sposoby ich wyeliminowania,
13. Raporty będą wykonywane każdorazowo na szablonach, które zostaną przedstawione przez Wykonawcę oraz po akceptacji tych szablonów przez Zamawiającego.
14. **Kompetencje osób wykonujących testy bezpieczeństwa.**
15. Zespół realizujący testy bezpieczeństwa musi składać się z nie mniej niż 2 osób
o kompetencjach opisanych poniżej,
16. Osoby wykonujące zlecenie muszą posiadać co najmniej średnie wykształcenie, a także posiadać aktualne kompetencje merytoryczne potwierdzone według następujących zasad:
17. co najmniej jedna osoba w zespole co najmniej dwuosobowym powinna posiadać kompetencje potwierdzone co najmniej jednym z certyfikatów: CISA (aktualnym i wydany przez isaca.org) lub CISSP (aktualnym i wydanym przez ISC2.org) lub Audytor Wiodący normy ISO 27001 (aktualnym i wydanym przez akredytowane organizacje certyfikujące) oraz jednym z certyfikatów eWPTv1 lub WAPTXv2 (wydanym przez eLearn Security – elearnsecurity.com) lub CMWAPT (wydanym przez IACRB – iacertification.org) lub CEH (wydanym przez EC-Council)

oraz

1. wszystkie osoby w zespole co najmniej dwuosobowym powinny posiadać kompetencje potwierdzone jednym z certyfikatów: OSCP (aktualnym i wydanym przez Offensive Security) lub CPTE (aktualnym i wydanym przez Mile2.com) lub GIAC (aktualny i wydany przez giac.org).
2. W przypadku gdy co najmniej dwaj członkowie zespołu prowadzącego zlecone testy bezpieczeństwa posiadają certyfikat opisany w punkcie D.2.1, wówczas w procesie wyboru jest to dodatkowo punktowane.
3. W przypadku gdy co najmniej jeden członek zespołu oddelegowanego do realizacji zadania posiada doświadczenie w przeprowadzeniu testów bezpieczeństwa fizycznego, polegających na ocenie odporności podmiotu na próby nieautoryzowanego fizycznego dostępu do pomieszczeń, wówczas w procesie wyboru jest to dodatkowo punktowane i Wykonawca zobowiązany jest również do świadczenia usług, o którym mowa w pkt A.5., w przypadku decyzji Zamawiającego o chęci skorzystania z ww. usług.
4. W przypadku gdy co najmniej jeden członek zespołu oddelegowanego do realizacji zadania posiada doświadczenie w przeprowadzeniu audytu bezpieczeństwa fizycznego, polegającego na ocenie architektury systemu kontroli dostępu oraz ocenie architektury systemu nagrywania wizyjnego (telewizji dozorowej), wówczas w procesie wyboru jest to dodatkowo punktowane i Wykonawca zobowiązany jest również do świadczenia usług, o którym mowa w pkt B.7.,
w przypadku decyzji Zamawiającego o chęci skorzystania z ww. usług.
5. Zamawiający zastrzega sobie prawo do każdorazowej akceptacji składu osobowego zespołu prowadzącego zlecone testy bezpieczeństwa.
6. Zamawiający wymaga aby osoby oddelegowane przez Wykonawcę do realizacji zamówienia
i wskazane w ofercie Wykonawcy osobiście świadczyły usługi.